- Close Window
- Print This Page
- Expand All | Collapse All

PD-29440

PD Information

PD Number	00CZ969	Master	□
Position Title	IT Specialist (INFOSEC)	Cloned from Master	□
Servicing HR Office	Central Office	Standard	Regional
Service/Staff Office/Region	Office of CitizenServices&InnovativeTechnologies	Owner	Manuela Martinez
PD Status	Active	Series	2210
Pay Plan	GS	Supervisory Status	Non-supervisory (8)
Grade	13	FPL	GS-13
Position Status	Competitive Service (1)	FLSA	Exempt
I/A	Yes	Competitive Level	N001
Position Sensitivity	Non-sensitive (1)	Financial Statement	OGE-450
Drug Test	Position does not require drug test (L)	Occupational Category Code	Administrative (A)
Public Trust Indicator	Level 5 - Moderate Risk (5)	Keywords	Cybersecurity Data Element Code 541,000,000
Legacy - Classified By		Capstone Official	□
Classified By	Manuela Martinez	Classified On	10/14/2014
Vacancy Announcement Number		Job Analysis Attachment	□

Description

Description

This position description is designated with a Cybersecurity Data Element Code 541,000,000 updated based on requirements as indicated in the NICE Cybersecurity Workforce Framework: November 2, 2016. Code 541 = Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. Ccato 9/14/17

*** Added new cybersecurity coding and language as required by OPM. MM 9/14/2017.**

Risk level: Non-sensitive, Moderate Risk, MBI, Tier 2, requiring Investigation Form SF-85P per NCC determination on October 14, 2014.

IT Specialist (INFOSEC),
GS-2210-13

This position serves as an expert Information Technology (IT) Specialist (INFOSEC) within the General Services (GSA), Office of Citizen Services & Innovative Technology (OCSIT). As a recognized expert in information security principles and practices, the employee performs complex, sensitive, high-level IT work characterized by a high degree of difficulty and responsibility. The incumbent performs evaluations of risk and vulnerability assessments of cloud service providers (CSP) and agency planned and installed information systems, to formalize the processes, find efficiencies, and educate stakeholders.

Major Duties and Responsibilities

The incumbent represents FedRAMP in meetings with CSPs, departments and agencies, public organizations, etc., to resolve problems, develop joint policies and standards, analyze, selection and implement security solutions and exchanges information regarding areas of technical expertise. Develops CSP and Agency outreach communications in coordination with technical subject matter experts on the FedRAMP security assessment process.

As a recognized IT security expert, develops policies and procedures to ensure information systems reliability and accessibility to prevent and defend against unauthorized access to and disclosure of federal information and develops of security test cases to ensure CPSs are compliant with FedRAMP guidelines and security controls.

Assesses the processes for security reviews of security controls for CSP and agency system security plans, security assessment plans, security assessment reports and other documentation to ensure accuracy and completeness in compliance with the Federal Information Security Management Act (FISMA) of 2002, National Institute of Standards and Technology standards and guidance.

Monitors FedRAMP technical and management project tasks and CSP authorizations in-process, analyzes issues and problems. Recommends automated, technology-based solutions, manages changes and ensures the quality of program deliverables.

Performs assessment of CSP continuous monitoring activities including CSP deliverables and scan results. Identifies process and policies that would result in greater efficiencies in the process for these assessments.

Develops and reports relevant metrics and reports concerning security authorization processes.

Participates in short and long-range program planning activities that include information security guidelines including NIST 800-53 and FISMA regulations, guidelines and standards. Performs professional work in policy development, strategic planning, evaluation, and problem identification and resolution.

Ensures that the FedRAMP activities and IT technical standards and guidelines are accomplished in accordance with prescribed federal laws, standards, policies, and regulations by writing appropriate instructions and guidelines.

Provides guidance on a broad range of IT security issues including computer security and technical standards to managers, and IT security specialists.

****Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.**

Performs other related duties as assigned.

Factor 1, Knowledge Required by the Position FL 1-8 1550 points

Mastery of and skill in applying advanced information technology (IT) concepts, principles, methods, industry standards and practices to develop and interpret policies; to provide expert technical advice and guidance on critical IT issues, and to apply new developments to problems, which involve ensuring the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools.

Mastery of IT security concepts, standards and methods and project management principles, methods and practices to address and manage a diverse array of IT issues and projects.

Expert knowledge of and experience developing, implementing, monitoring, and reporting on the elements of information security management programs. The employee has knowledge sufficient to implement effective planning and reporting, implement security awareness programs, and ensures adequate training for technology users.

Expert knowledge of IT security certification and accreditation requirements sufficient to provide advice and guidance to management in implementing IT security policies and procedures in the development and operation of network systems. Knowledge of new IT and security developments sufficient to advise management on the need for system modifications and upgrades and other IT recommendations of significant importance to the serviced organization.

Expert knowledge of computer forensic principles sufficient to ensure proper development of evidence used in investigating breaches of IT systems and data security.

Expert knowledge of the latest threats and vulnerabilities, vulnerability scanning tools, and other continuous monitoring tools (e.g., TCP/IP, routing protocols, subnet, access control list, firewall, router, switch, VPN, load balancer, network traffic analysis, IDS/IPS, proxy, etc.) in order to recommend new or revise security measures and countermeasures.

Knowledge of communication and negotiation techniques sufficient to establish and maintain effective working relationships across GSA and with representatives of other Federal, State and local governmental agencies, intermediaries, service carriers, and private sector organizations.

Knowledge of, and skill in applying, IT security principles and methods; analytical ability; and communications techniques sufficient to update the organization’s contingency or disaster recovery plans to respond to new security requirements or changes in the IT architecture; and present updated plans to the IT security manager for review and approval.

Knowledge of, and skill in applying, systems security principles and methods; and systems security regulations and policies sufficient to develop specifications to ensure compliance with security requirements at the systems level.

Ability to communicate complex and highly technical ideas both written and verbally in order to formulate and present findings, briefings, project papers, status reports, and correspondence to foster understanding and acceptance of findings and recommendations.

Factor 2, Supervisory Controls FL 2-4 450 points

The supervisor outlines overall objectives and key priorities. The employee independently plans own work, coordinates with team members or other IT specialists, resolves most problems that arise and carries assignments through to completion. For unusually difficult, complex, controversial or state of the art projects, the employee advises the supervisor of potential problems, accompanied by a proposed plan of action. The work is reviewed for effectiveness in meeting requirements and soundness and feasibility of recommendations.

Factor 3, Guidelines FL 3-4 450 points

Guidelines include technical manuals, policies and directives; IT regulations, and industry standards. Guides are very general in nature and require considerable interpretation and/or adaptation for application to issues and problems. The employee uses judgment, initiative and resourcefulness in deviating from established methods to modify, adapt and/or refine broader guidelines, and to develop new methods, policies and/or practices for the IT organization.

Factor 4, Complexity FL 4-5 325 points

The work involves the performance of risk and vulnerability assessments of cloud service providers (CSP) and agency planned and installed information systems, to identify vulnerabilities, risks and protection needs. The employee assesses effectiveness of installed systems, implements modifications to minimize vulnerabilities, troubleshoots security threats and vulnerabilities in response to incident reports, identifies and isolates problem sources, and recommends solutions or corrects problems. The employee anticipates needs for change to avert potential systems, data, or network vulnerabilities. The employee is responsible for the technical correctness of methods and techniques used, and must gain management acceptance of more restrictive IT policies, when required. The work requires coordination and evaluation of programs and structures to ensure security and identify potential problems. The employee implements changes to ensure the organization is compliant with higher level policy directives. The work also consists of a variety of duties requiring the application of many different and unrelated processes and methods to the in-depth analysis of IT security issues that require significant departure from standard practices and procedures to resolve critical IT security issues. He/she participates in joint efforts to develop policies and standards, analyzes, selects, and implements security solutions and exchanges information regarding areas of technical expertise. In consultation with the cloud service providers, federal agencies and workgroups the employee defines overall IT security and functional requirements; plans and coordinates systems design, implements, and analyze and resolves a wide range of IT security issues and problems. The employee makes decisions that involve major uncertainties with regard to the most effective approach or methodology to be applied, such as changes typically resulting from constantly changing customer requirements and/or rapidly evolving technology in the specialty areas. The employee develops new standards, methods and techniques; evaluates the impact of technological change, and/or conceives of IT security solutions to highly complex technical issues.

Factor 5, Scope and Effect FL 5-4
225 points

As a recognized IT security expert, the purpose of the work is to develop policies and procedures to ensure information systems reliability and accessibility to prevent and defend against unauthorized access to and disclosure of federal information and develops of security test cases to ensure CPSs are compliant with FedRAMP guidelines and security controls The purpose of the work also includes providing IT technical expertise in specialized security areas to ensure data and systems security. The work involves conducting assessments of threats and vulnerabilities, and determining deviations from acceptable configurations or enterprise or local policy, selecting, installing, and monitoring the performance of appropriate security tools, including firewalls, intrusion detection systems, and vulnerability of self-assessment programs, troubleshooting IT security problems that affect the availability of agency IT systems and recommending actions that will minimize risks, and developing and implementing policies and procedures to ensure systems and data protection. The work ensures the protection of IT assets and affects the ability of cloud providers to ensure that their infrastructures are secure and that data is protected. It also affects the ability of federal customers to ensure that the providers have taken the proper security measures to protect their information.

Factors 6 & 7, Personal Contacts and Purpose of Contacts FL 3C
180 points

In addition to the everyday contacts with work group members, peers, and higher management, the employee contacts Federal, State, and local governmental agencies, GSA contractor personnel, top technical and management personnel. These contacts occur at worksites and offsite locations. Contacts are frequently with top-level IT personnel and higher level management officials.

Contacts are for planning and coordinating major IT projects and initiatives, often requiring extensive negotiations. Contacts are also for the purpose of providing technical guidance, resolving controversial problems and conflicts, and recommending technical solutions which are beneficial to cloud providers and cloud consumers. The employee must be skillful in approaching contacts to obtain the desired effect (e.g., gaining compliance with established policies and regulations by persuasion or negotiations).

Factor 8, Physical Demands FL 8-1 5 points

The work is sedentary; may have to carry light items, such as papers, books or small parts. Some travel may be required. Some work may require walking and standing in conjunction with travel and to attend meetings and conferences away from the work site.

Factor 9, Work Environment FL 9-1 5 points

The work is performed in an office setting that is adequately lighted, heated, and ventilated, with no environmental stresses. The work environment involves everyday risks or discomforts that require normal safety precautions.

Total Points: 3190
GS-13 Point Range: 3155 - 3600

Reference: OPM Job Family Standard for Administrative Work in the Information Technology Group, 2200, revised May 2011 and General Supervisory Guide, dated June 1998.

Final Classification Determination: IT Specialist (INFOSEC), GS-2210-13.

FLSA EVALUATION

Computer Employee Exemption

Met – Salary Threshold. Base pay for this position exceeds $23,660 per annum or if paid hourly, $27.63 per hour; AND
Met – Primary duty consistent with 5 CFR 551.104 (e.g.; non-manual work directly related to the management or general business operations of the employer or its customers); AND
Met – Primary duties involve the analysis, design, and/or development of computers systems and programs as defined in 5 CFR 551.210.
Comments/Explanations: As a recognized expert in information security principles and practices, the employee performs complex, sensitive, high-level IT work characterized by a high degree of difficulty and responsibility. The incumbent performs evaluations of risk and vulnerability assessments of cloud service providers (CSP) and agency planned and installed information systems, to formalize the processes, find efficiencies, and educate stakeholders. The duties assigned to this position are consistent with 5 CFR 551.210(b) thus meeting the criteria for the Computer Employee Exemption.
Conclusion: Exempt.

Additional Description

Created By	Manuela Martinez, 10/14/2014 7:39 AM	**Last Modified By**	Cheryl Cato, 10/14/2018 8:26 PM